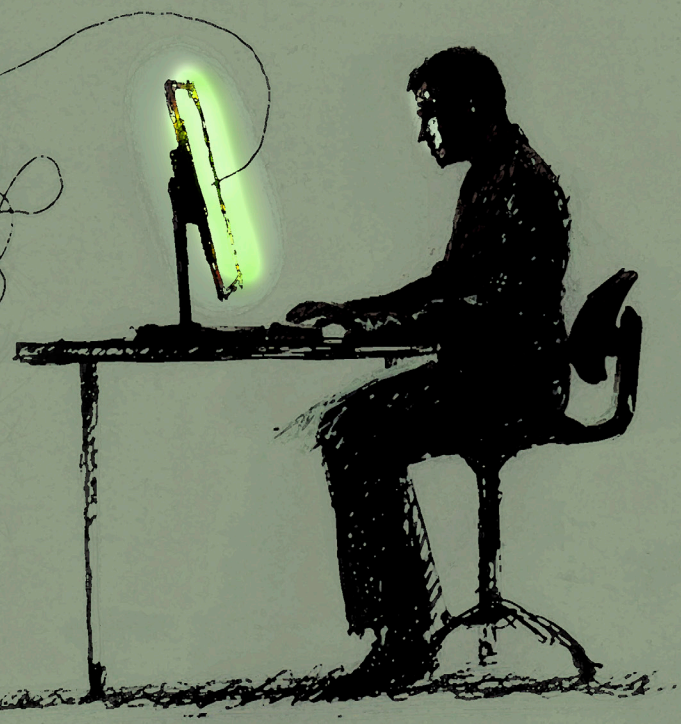
Putting threat intelligence into context

Are threats being hidden by too many distracting threat feeds?



ebook

An SC Media publication

Sponsored by

NETSCOUT®

Arming your infosec staff intelligently

Too much intelligence data that is poorly managed can obfuscate real threats. Without having a handle on the context of the intelligence, data feeds could make you overlook the threats within. Evan Schuman explains.

In the world of threat intelligence, context is everything. Without context for data feeds, log files and open source intelligence, some experts fear the data and the respective feeds are not merely pointless — an ocean of noise drowning out the serious threat signals — but can literally distract security teams and make the enterprise less secure.

There is a growing concern that far too many CISOs are accepting this avalanche of data without imposing the proper contextual backgrounds, and that can mean the difference between your security team improving their collective skills to keep you more secure or simply drowning in data points.

Understanding what you need, what you have, and how it all fits together is the Rubik's Cube of taking cybersecurity to the next level. The context of the intelligence helps companies differentiate between real threats, such as multiple reports from Information Sharing and Analysis Centers (ISAC) of similar attacks on multiple companies in the same industry at the same time on the same day from scattered reports of potential ransomware attacks where there is no data to indicate that the same attacker is attacking specific targets. Bringing order to the random data from data feeds and log files is one way to define context, experts agree.

Bringing order from disorder

Paul Hill, a senior consultant with SystemExperts, an IT security consulting firm located near Boston, says the nature of most compiled threat feeds use inconsistent references and other problems that make the data problematic. He offers real-life examples of how threat intelligence data, no matter how valuable, can be devalued effectively in an environment where the security staff simply has not evolved its operations to meet the growing problem — or its solution.

A company "might have all of the information, but it is too partitioned to make actionable plans," Hill says. "Unfortunately, there is so much information generated by vendor notifications, the CISA (Cybersecurity and Infrastructure Security Agency), and the NVD (National Vulnerability Database), that few organizations have the staff to keep up with the information flow."

Hill, for example, describes what he observed at one of his enterprise clients where they had, in Hill's words, "an infrastructure and ingrained segregation of duties that hindered security investigations and delayed remediating issues."

Among the problems, according to Hill: "Some audit logs included the public IP address of a device, but other audit log sources gave the internal NAT (network address translation) IP address, and the SOC (security operations center) staff were not provided with any tools to map public IP addresses to

OUR EXPERTS: Threat Intelligence

J. Eduardo Campos, security specialist, Embedded Knowledge Inc.
Scott Caschette, CIO, Schellman & Company
Geoff Hauge, partner, Edgile consulting
Paul Hill, senior consultant, SystemExperts
Michael Sechrist, cyberthreat intelligence team lead, Booz Allen Hamilton
Umesh Yerram, chief data protection officer, Amerisource Bergen

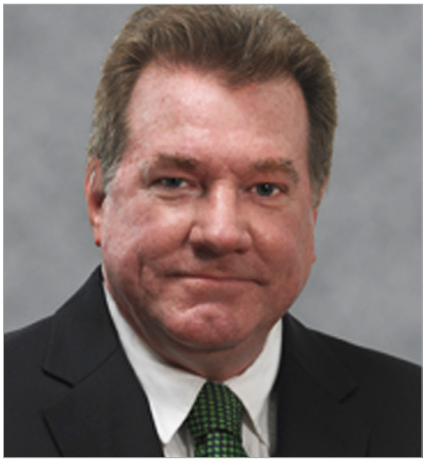
52%

Percentage of companies that view IT infrastructure as one of the biggest challenges of supporting AI initiatives

– ESG

NAT IP addresses. Instead, the SOC team had to ask the network infrastructure team about individual IP addresses via email or IM (instant messenger).

"The SOC team did not have the ability to reverse query an IP address in order to determine the DNS name of the system," he continues. "Instead the SOC team had to ask the network infrastructure team about individual IP addresses. While the organization had multiple automated asset inventory systems, the SOC staff were not granted the ability to query or generate reports from the asset inventory systems. A request had to be made to either the server operation team or the desktop support team for individual IP addresses or system names."



Paul Hill, senior consultant, SystemExperts

Hill adds: "The data centers were outsourced to a large colocation facility that also functioned as a managed security service provider (MSSP), including the management of firewall rules, IDS (intrusion detection system) alert rules, and IPS (intrusion prevention system) rules. The SOC staff was not provided with a point of contact at the colocation facility. Instead, all inquiries and configuration requests had to be submitted to the infrastructure team which would in turn submit them to the colocation provider."

> "The data that comes in is rather sterile. It's binary data, factual data, but it's still sterile. It has a lack of context or opinion."
>
> *– Scott Caschette, CIO, Schellman & Company*

J. Eduardo Campos, an author and the founder and president of the consulting firm Embedded-Knowledge Inc. in Bellevue, Wash., points to poor company-units-to-security communication as an important challenge for threat intelligence. The threat feeds detail lots of external security situations, but companies are being hit every day with attacks, both cyberattacks and social engineering trickery attacks.

Campos points to those social engineering attacks as ones where communication often breaks down. Let us say a thief is trying to trick employees into revealing security credentials. The attacker makes dozens of calls to your call centers and business units and anyone else they think might have those credentials. If your people are well trained, most of those efforts will fail, he notes.

But what happens when the attempt fails? Do your people immediately call or message security, telling them of the attempt? In Campos' experience, the answer is that they almost never do. If those calls happened right away every time, security could message all employees with a description of the con and make it even less likely to succeed. Few security departments ever get that chance because employees do not bother to call if the attempt fails. And they are scared to death to call if the attack succeeds.

"If you're not considering what your front managers are seeing because you don't have a structure to capture it," that is a problem, Campos says. Companies need to create better reporting mechanisms. As things stand today, "the LOB (line of business) is going to complain or they are just going to ignore you. Give them a hotline to call." Alternatively, take a page from DevSecOps and cross pollinate security people through every

$12B

AI and machine learning revenue are expected to drive the security analytics market reach to $12 billion by 2024.

– ABI Research

business unit or just train one person in those units to know what security needs to hear.

"Create a sense of community. Offer awards for those employees who are better at spotting these phishing attacks. We take the users for granted. You need to find ways to connect to people. That's what is missing," Campos says.

Campos also says the cloud is both a source of good security information as well as a potential source for more security holes. "You have to test all the time, especially for hybrid environments," he says, acknowledging that just about every Fortune 1000 enterprise has hybrid cloud to various degrees. Sometimes cloud tech teams will make setting changes "and they are forgetting to let the CISO know. You need to know what is at the edge of your network."

Normalizing data feeds

While the term 'data feeds' can be defined differently by each vendor, they often contain several common components. Among those components are data sources from commercial and private data intelligence firms; data from publicly available open sources such as social media, company websites, news organizations and the like; information taken from deep and dark web sources; website scanners and scrapers; bulletins from vendors, consultants and others; the company's own security information and event management (SIEM) systems; and other internal sources. Additionally, some companies add data from honeypots, sinkholes, botnets, and monitor systems.

Data is good and more data is better, right? Not necessarily, says Geoff Hauge, a partner in the Austin-based consulting firm Edgile. Earlier, Hauge was the CISO for Santander Bank based in Spain, with some $75 billion in assets and about 600 branches in eight northeast U.S. states. He also served as well as the division information security officer for the Royal Bank of Scotland, which has total assets of £700 billion.

"The downside [to massive amounts of intelligence data] is that it absolutely can be a distraction and add to the sensory overload for organizations that don't have the proper security platform to handle the data," he says. The failure he sees frequently are large enterprises that sign up for multiple, high-quality threat feeds, but they drop the ball when it comes to customizing that data for their own business, their vertical, their geographies, and their specific security defenses. The original intent for threat feeds was for them to be generic and then made specific by the work of salaried security analysts for that business. But, Hauge says, he sees far too many companies using the feeds as is.

> "I believe the next evolution in TI space will be gaining understanding of who are the threat actors that are attacking a particular organization and how."
>
> *– Umesh Yerram, chief data protection officer, Amerisource Bergen*

These enterprise security operations "take no action, provide no context, to tell if their threat exposure has increased or decreased. He offered an analogy of the $400,000 advanced war fighter helmet that provides fighter pilots a line of sight and it displays all relevant information and, critically, hides anything irrelevant or distracting. What he sees too many enterprise CISOs doing today is "the equivalent of giving the pilot a report and saying, 'Read this while you fly the plane.'

"Most [CISOs] don't even have a current asset inventory, which means they don't have the foundation to get started," Hauge

>33B

By 2023 more than 33 billion items of data will be stolen by cyber criminalss

– BOHH Labs

continues. "If you don't have the assets or the capabilities, you're just creating additional sensory overload. Sometimes, this provides the illusion that you're more advanced than you are. They don't have the ability to act on it and they don't know how it impacts their environment."

Geoff Hauge, partner, Edgile consulting

Often, Hauge will tell CISOs, "Show me one tactical change you made based on that report. More often than not, it makes them feel that they look good. It may be for a regulator, to say 'Look, we've acquired this advanced intelligence feed.' They are much better off working with their ISACs and getting better knowledge-sharing. [The feeds] should reduce the number of events that they are looking at. If it's not doing that, it's just sensory overload."

Scott Caschette, the CIO for Schellman & Company, a security and compliance assessor based in Tampa, Fla., agrees with Hauge's take but stresses that the global context is potentially more important than vertical or U.S. context.

"Cybercrime recognizes no borders, language or culture. The net effect of that fact is a dizzying array of incongruent laws and penalties that feel like 'pushing a rope' when it comes to enforcement. We are out-manned and out-gunned and the divide between skilled workers and effective tools continues to widen every day, painting a somewhat grim picture of the future," Caschette says.

"Cybercriminals are organized, quick to react, nimble and operate with little to no risk. Meanwhile we continue spending exorbitant amounts on technologies, internal staff and threat intelligence which are only treating the symptoms and not the root cause. Of course we need firewalls, endpoint security, SIEM, training and all of the usual suspects in defending against cybercrime, but until we treat the root cause we will continue to lose the battle and the war," he continues.

"Collaboration and threat intelligence sharing are largely useless unless applied to sophisticated tools that have global visibility, can correlate real-world events, intent, predictive analytics, and ultimately produce evidence of criminal activity," he continues. "Treating the root cause in our case is vaccinating against the overwhelming risk/reward ratio that cybercriminals operate in. In countries where an average worker with access to technology makes around $18,000 a year, the prospect of easily making $500,000 or more per year with no risk is pretty appealing."

Caschette's answer is for a massive increase in global information sharing, common penalty frameworks and cross-border laws that are clear and severe to anyone considering a life of cybercrime.

"Although this might seem like an arduous task to get all nations on Earth to coordinate and build a common threat intelligence, information sharing and penalty framework," he says, "I would present the example of the airline industry. Each airline operates autonomously, sharing common systems, rules, polices, costs and frameworks with every other airline and nation on the planet. It's time to go on the offensive and get serious about establishing not only better intelligence sharing, but also better deterrents."

But regardless of whether the context is global or domestic, Caschette agrees with Hauge that the threat feeds most enterprises depend on today are being used either without context or with woefully inadequate context.

"The data that comes in is rather sterile.

55%

Percentage of SMBs that are willing to pay a ransom to recover encrypted data or to prevent it from being shared

– AppRiver 2019 Cyber-threat Index for Business Survey Report

It's binary data, factual data, but it's still sterile. It has a lack of context or opinion," Caschette says. "Any of the data that is coming in you should be correlating against real-world events."

Scott Caschette, CIO, Schellman & Company

Not everyone sees the issue as solely one of external context. Umesh Yerram is the chief data protection officer at AmerisourceBergen, the $168 billion healthcare Chesterfield, Pa.-based concern that ranks in the Fortune 500 Top 10. Yerram sees a lot of those threat intelligence data feeds as having quality issues on their own, regardless of whether an attempt is made at getting more context.

Yerram argues that companies can subscribe to hundreds of different feeds — some open source, some paid — and it is hard to know the good ones from the bad ones.

"There is a TI [threat intelligence] overload for security teams. The TI market today is so saturated that the key question is fidelity of those TI reports. Does the TI feed source have the required technical security and industry SME expertise to address potential accuracy issues?" Yerram says. "For instance, some feeds have low accuracy stemming from a large proportion of CDN (content delivery networks) and non-routable IP addresses included in the feed, which often makes [them] much less actionable. Therefore, quantity does not equate to quality."

Just as importantly, though, Yerram says, is that CISOs and CSOs use the feeds properly.

"Many organizations use TI as a point-in-time validation to determine whether the threat exists within their environments. Organizations should go beyond the traditional view of threat intelligence as consuming threat feeds, hashes, domains, pastebin code, IP addresses, or Yara rules, and also look into indirect threat intelligence, understanding the consequences and the related strategic and tactical operational actions stemming from TI," Yerram says.

"I believe organizations should use that TI to assess and test whether their defenses are well equipped to block or detect those threats if attackers target their enterprise," he continues. "Furthermore, fine-tune their defense and detection capabilities and determine what their response strategy will be when that threat is detected in the environment."

Yerram also agrees with Hauge and Caschette that CISOs must add localization and customization context to the feeds, to make them actionable and relevant to their enterprises. Yerram specifically adds supply chain particulars to that customization.

"TI subscription feeds are, at the most, specific to industry but never customized to one organization's security or threat posture. Organizations cannot fight threats coming at them with a blindfold on, such as not knowing who are the motivated threat actors determined to attack them and how," Yerram says.

"I believe the next evolution in TI space will be gaining understanding of who are the threat actors that are attacking a particular organization and how. APT10 or APT31 or Fancy Bear is not targeting everyone, as we know, but knowing who is trying to launch attacks and how and when will definitely be a game-changer. Today," he says, "there is so much noise from the existing intelligence, so many false positives."

Mergers and acquisitions

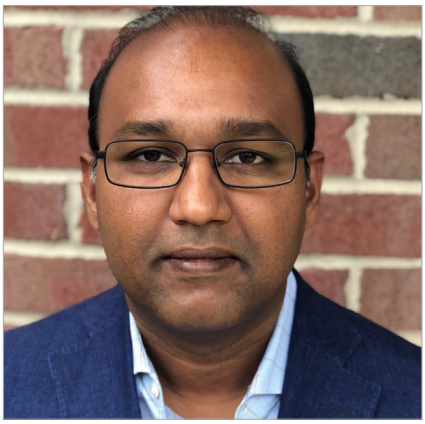
Another item that many threat intelligence experts says concerned them was mergers and

£4.5B

Annual cost to small businesses in the UK face from the nearly 10,000 cyberattacks they face daily

– The Federation of Small Businesses

acquisitions (M&A) protocols involving security, specifically including the CISO's team in extensive due diligence efforts of companies before it is deciding if an acquisition will proceed. Although it is now starting to happen with some enlightened enterprises, far too many either neglect to bring in security until it is much too late in the process to back off the acquisition or they do not bring security in at all until the acquisition is finalized.



Michael Sechrist, cyberthreat intelligence team lead, Booz Allen Hamilton

When it comes to the risk around enterprise merger and acquisitions strategies, the complacency is less about what security personnel do or do not do, but is entirely about whether the CISO can afford to be complacent about nagging, begging and insisting that proper investigations be done early enough to make a difference.

Specifically, it is about nagging, begging and insisting to the CFO, who typically is in charge of due diligence efforts on new acquisitions. Security needs to do full-fledged due diligence, from penetration testing the potential firm being acquired to interrogating their cloud host to reviewing their regulatory and industry compliance status and generally learning everything about their threat profile.

That insistence must be that investigating the company after-the-fact — say, perhaps, after a letter of intent is signed by all but before a deal is closed — might well be too late to identify security vulnerabilities whose costs to mitigate could turn the tide on the entire investment. The CFO needs to hear privately from security about the additional costs that this acquisition could force your team to spend to defend these new people.

Yerram argues that security must thoroughly review the threat situation of any potentially acquired company. CISO teams must "fully assess the environment" of the potential to-be-acquired company, he says. "Are they up-to-date on patching?" At Amerisource Bergen, Yerram says, "we are a very integral part of the M&A playbook" and they conduct industry compliance as well as penetration testing/intrusion assessment of all serious candidates.

With mergers and acquisitions efforts, it is not solely concerns about security holes that the new company might bring to the acquiring enterprise, it can also be an issue of whether that acquisition will bring with it a different kind of attacker. For example, an enterprise might be used to defending against routine cyberthieves and identity thieves, but if the potential acquired company has military contracts, that acquisition could bring along with it state actors: highly-financed and well-equipped agents working for China, Russia, North Korea or other governments. Fighting state actors requires a very different — and often a far more expensive — defense strategy.

There are also the routine issues of overlapping or duplicative software licenses, especially with SIEMs. Sometimes someone from security needs to tell the people in the CFO's office a lot of the security-related costs that they might not have calculated.

Conducting due diligence on a company being acquired without analyzing the IT implications can lead to significant complications with both organizations' staffs and IT systems. Complacency on the part of the IT staff, especially when it comes to merging SIEM environments, as well as the aforementioned new class of potential attackers, could lead potentially to high and unanticipated costs if a company assumes that SIEMs and other systems will work seamlessly with those of newly acquired

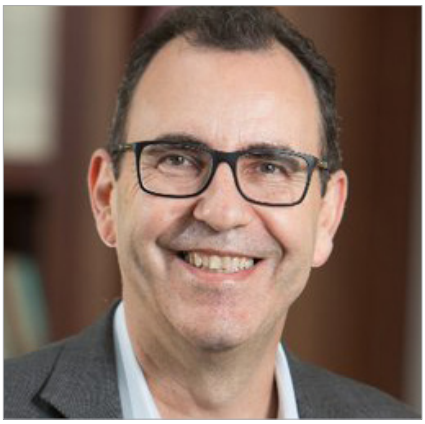
36%

Percentage of organizations that cite data integration as an analytics technology or process that has given them the most difficulty

– ESG

companies and that appropriate defenses are in place for the new threat profile.

Art Langer, director of the center for technology management at Columbia University, argues that threat intelligence needs to be weaved better into overall threat defenses. To that end, he argues for a far more robust — and faster — path to DevSecOps than most companies are, thus far, comfortable to do.



J. Eduardo Campos, security specialist, Embedded Knowledge Inc.

"CISOs tend to behave outside the realm of architecture in the software development process, and that has to change — they can no longer be separate from the design process. Threats act like the flow of water, they follow the path of least resistance. So just because a threat can't get through one safeguard doesn't mean it won't continue trying until it gets in," Langer says. "In order to protect assets from persistent threats, CISOs need to completely transform their roles to be involved in the design of systems, building their knowledge of threat intelligence from the inside out. Few, if any, are doing that now, and CISOs who aren't are playing a losing game."

> "TThere are some attackers who are looking for data that you had no idea about. [CTI analysts] are the ones who have a good sense; they are the eyes and ears on the external threats."
>
> *– Michael Sechrist, cyberthreat intelligence team lead, Booz Allen Hamilton*

A longtime threat intelligence specialist is Michael Sechrist, who today leads the cyberthreat intelligence team at consulting firm Booz Allen Hamilton. Before Booz Allen, Sechrist held a variety of corporate, academic and government security roles, including serving as the special assistant to the undersecretary at the U.S. Department of Defense, Special Assistant to the Under Secretary for Arms Control and International Security at the U.S. State Department, and Department Associate Director at The White House.

Sechrist encourages enterprise CISOs to make sure that they use plenty of open source threat feeds in addition to commercial sources, to get a rounder view of the various threat environments. It is also critical, he says, to bring CTI (cyberthreat intelligence) analysts into the process.

"There are some attackers who are looking for data that you had no idea about," he says. "[CTI analysts] "are the ones who have a good sense; they are the eyes and ears on the external threats."

Sechrist argues that focusing on any one area — including CTI analysts — limits the global view of threats too much.

"If you grow this organically out of a CTI division, they immediately run into obstacles and silos of information. You need access to so many other things to understand the likelihood of a threat and its impact in a company," Sechrist says. He advocates a much more comprehensive approach, such as the Intelligence Lifecycle (IL).

"Don't create IL just within the purview of a CISO or threat intel manager. Create an enterprise IL function that has the purview to pull in many different data sources," he continues. "A good IL should sit within the enterprise risk division, which tends to have a broader purview to pull in data sources and evaluate the things like the actual legal

43%

Percentage of robocalls that are considered spam

– YouMail

structure of the company, IT connections from network to network, planned M&A. Many CTI analysts have an external focus but to become a good intelligence analyst, you have to understand your company, be able to look across all sorts of business lines and know how the company operates."

Michael Sechrist, cyberthreat intelligence team lead, Booz Allen Hamilton

Sechrist also pointed to a very serious problem with threat intelligence, which is simply an ominous side effect of the "punish the messenger" tactic. That is where senior security management makes the person who reports a problem the one who has to fix it, which ends up discouraging reporting, especially if the analyst is already overworked, which they all are — or at least they all believe they are.

"Many companies create a conflict of interest for their intelligence analyst by making them the person who needs to report on a threat and fix it. For example, you're an intelligence analyst reporting up to your CISO about a significant threat and [the CISO] asks, 'How do you recommend we fix this?' The [analyst] might say, 'We need to quickly fix a large-scale IT problem that has existed for years' and the CISO's response might be, 'You know how to fix it [so] you go do it.'

"In that scenario," he notes, "you've taken the intelligence analyst off the other work they've been doing and turned them into someone who now must fix something they reported on. This creates a situation where what actually gets reported [is compromised] because intelligence analysts worry they'll put themselves in a position where they have to fix a problem and also explain why they weren't covering/providing intelligence on another threat. Not disassociating these two tasks can put even bigger strains on intelligence teams than companies are aware. It's why intelligence analysts are turning into Swiss Army Knife digital responders. Companies might be shooting themselves in the foot by putting so much stock or work on one team," Sechrist says. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

18%

Percentage of companies that are storing all of their privileged accounts in a secure PAM vault or password manager

– Thycotic